UN privacy watchdog says 'little or no evidence' that mass surveillance works

The laws are "predicated on the psychology of fear," which prevents the public from "objectively assessing the effectiveness" of privacy-busting measures, said the UN special rapporteur.


The United Nations' special rapporteur on privacy has lambasted a spate of new surveillance laws across Europe and the US, saying that there is "little or no evidence" that mass monitoring of communications works.

In a report published this week, Prof. Joseph Cannataci, the first privacy watchdog to take up the post, said he was neither convinced of the effectiveness or the proportionality "of some of the extremely privacy-intrusive measures that have been introduced by new surveillance laws."
He also said that bulk records collection, such as call and email metadata, runs the risk of "being hacked by hostile governments or organized crime."

Cannataci singled out recently-passed laws in France, Germany, the UK and the US, all of which have pushed through new legislation in the wake of the threat from the so-called Islamic State.

He said that the passed laws amount to "gesture-politics," which in his words, "have seen politicians who wish to be seen to be doing something about security, legislating privacy-intrusive powers into being -- or legalize existing practices -- without in any way demonstrating that this is either a proportionate or indeed an effective way to tackle terrorism."

A rise in public support of increased surveillance powers is "predicated on the psychology of fear," he said, referring to the perceived threat of terrorism.

The report is one of the more critical analyses in recent years on the global surveillance apparatus, which was in part disclosed by documents leaked by Edward Snowden.

Those documents put a spotlight on domestic and international monitoring of calls, messages, and the hacking capabilities of the US National Security Agency and other members of the so-called Five-Eyes alliance of nations.

Since the revelations, there has been some push-back in the US -- notably the Freedom Act (http://www.zdnet.com/article/freedom-act-metadata-phone-records-prism/), designed to limit bulk collection of phone and email records -- but other nations have headed in the opposite direction.

Both France (http://www.zdnet.com/article/europes-answer-to-terror-attacks-on-free-speech-is-to-double-down-on-internet-censorship/) and Germany (http://www.zdnet.com/article/germany-moves-closer-to-data-
UN privacy watchdog says 'little or no evidence' that mass surveillance... have pushed for great surveillance powers following terror attacks, allowing for police and intelligence agencies to monitor internet activities and call records.

And, the UK late last year pushed through (http://www.zdnet.com/article/snoopers-charter-expansive-new-spying-powers-becomes-law/) the "most extreme surveillance law ever passed in a democracy," according to Jim Killock, director of the Open Rights Group.

In a final recommendation, Cannataci said governments should "actively explore" how to carry out fair and regulated surveillance while balancing the introduction of privacy-friendly safeguards.

"This would not only be of great intrinsic value to citizens worldwide but would also send a clear signal to those states, democracies, pseudo-democracies and otherwise who mistakenly believe that the best way to deal with cyberspace is to claim sovereignty over chunks of the Internet or what its citizens get up to on the Internet," he said.

"Human rights are universal and cyberlaw should exist in such a way not only to protect privacy but also other fundamental human rights," he added.

**VIDEO: Easily hacked IoT devices can turn a university’s network against itself**

**ZDNET INVESTIGATIONS**

US government pushed tech firms to hand over source code (http://www.zdnet.com/article/us-governmentpushed-tech-firms-to-hand-over-source-code/)

At the US border, expect discrimination, detention, searches, and interrogation (http://www.zdnet.com/article/welcome-to-the-united-states-discriminated-detained-searched-interrogated-special-report/)


Meet the shadowy tech brokers that deliver your data to the NSA (http://www.zdnet.com/article/meet-the-shadowy-tech-brokers-that-deliver-your-data-to-the-nsa/)

Trump aides’ use of encrypted messaging may violate records law (http://www.zdnet.com/article/trump-aides-use-of-encrypted-messaging-verges-on-violating-records-law/)

An unsecured database leaves off-the-grid energy customers exposed (http://www.zdnet.com/article/off-the-grid-thousands-exposed-after-database-leak/)

Inside the global terror watchlist that secretly shadows millions (http://www.zdnet.com/article/inside-the-global-terrorism-blacklist-secretly-shadowing-millions-of-suspects/)
Security flaws in Pentagon servers "likely" under attack by hackers (http://www.zdnet.com/article/pentagon-system-flaws-likely-under-attack-by-foreign-hackers/)

Revealed: How one Amazon Kindle scam made millions of dollars (http://www.zdnet.com/article/exclusive-inside-a-million-dollar-amazon-kindle-catfishing-scam/)